6. Field Extensions

Field Extensions

Splitting Fields (Normal Extensions)

Definition

Definition: Let $f(x) \in F[x]$ be a polynomial and let K/F be an extension field. K is called a *splitting field* for $f(x)$ if

- f splits into linear factors in K
- f does *not* split into linear factors over any proper subfield of K.

Splitting fields exist

Proposition: Any polynomial $f(x) \in F[x]$ has a splitting field.

Proof: If all irreducible factors of $f(x)$ have degree 1 then F is a splitting field. Otherwise, let α be a root of an irreducible factor of f of degree greater than 1 and let $F_1 = F(\alpha)$. Write $f(x) = (x - \alpha)f_1(x)$ and, by induction, let E be a splitting field for $f_1(x)$ over $F(\alpha)$. Then all the roots of $f(x)$ belong to E. Let K be the subfield of E generated over F by the roots of $f(x)$. This is your splitting field.

Remark: Some books say that if K/F is the splitting field over F for a polynomial, then K is called a normal extension.

Degrees of splitting fields

Proposition: If $f(x) \in F[x]$ has degree n then its splitting field has degree at most $n!$.

Proof: It can be obtained by adjoining roots successively of polynomials of degree n, $n-1$, $\ldots$.

Examples

1. $f(x) = (x^2 - 2)(x^2 - 3)$. Splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ which has degree 4.

2. $f(x) = x^3 - 2$ which is irreducible by Eisenstein. Three roots are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ where $\omega = e^{2\pi i/3}$ is a cube root of one. Since

$$\omega = \frac{-1+\sqrt{-3}}{2}$$

this field has degree six and contains $\sqrt{-3}$.
3. x^4+4 "looks irreducible" but it isn't. It factors as $(x^2+2x+2)(x^2-2x+2)$. It splits over the field $\mathbb{Q}(i)$ because $(\pm 1 \pm i)^2 = \pm 2i$ so $(\pm 1 \pm i)^4 = -4$.
4. The splitting field of $x^n - 1$ is called the n^{th} cyclotomic field and is generated by $e^{2\pi a/n}$ where a is an integer relatively prime to n. If n is prime, then $x^p - 1$ then it factors as $(x-1)(1+x+\cdots+x^{p-1})$; the second factor is irreducible so that field has degree $p-1$.
5. The splitting field of $x^p - 2$ has degree $p(p-1)$.

Uniqueness of splitting fields

Extensions of isomorphisms

Theorem: (DF Theorem 27 p. 541) Let $\phi : F \to F'$ be a field isomorphism. Let $f(x) \in F[x]$ and let $f'(x) \in F'[x]$ be the polynomial obtained from f by applying ϕ to its coefficients. Let E/F be a splitting field of f and let E'/F' be a splitting field of f'. Then there is an isomorphism $\sigma : E \to E'$ which makes the following diagram commutative (the vertical arrows are the inclusion maps):

$$\begin{tikzcd} E \arrow[r, "\sigma"] & E' \\ F \arrow[u] \arrow[r, "\phi"] & F' \arrow[u] \end{tikzcd}$$

Corollary: Any two splitting fields for $f(x)$ are isomorphic via an isomorphism that is the identity on F.

More on extensions

The extension theorem can seem a little mysterious. Let's look more closely at an application.

Let $f(x) = x^3 - 2$ and let $E/\mathbb{Q}$ be its splitting field (which has degree 6 over $\mathbb{Q}$). Inside this field there are three isomorphic cubic extensions: $L_1 = \mathbb{Q}(\sqrt[3]{2})$, $L_2 = \mathbb{Q}(\omega\sqrt[3]{2})$, and $L_3 = \mathbb{Q}(\omega^2\sqrt[3]{2})$ where $\omega = e^{2\pi i/3}$ is a cube root of unity.

$$\begin{tikzcd}
 & E & \\
L_1 \arrow[ur] & L_2 \arrow[u] & L_3 \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Now E is a splitting field for $f(x)$ over each of L_1, L_2, and L_3.

Still more on extensions

We can apply the theorem to (for example) the diagram

$$\begin{tikzcd}
E \arrow[r, "\sigma"] & E \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[u] \arrow[r, "\phi"] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[u]
\end{tikzcd}$$

where ϕ is the isomorphism that sends $\sqrt[3]{2} \to \omega\sqrt[3]{2}$ and fixes $\mathbb{Q}$. It follows that there is an automorphism σ of the splitting field that extends ϕ.

Automorphisms of splitting fields of irreducibles

In general, if $f(x)$ is an irreducible polynomial over F, and α and β are two roots of $f(x)$ in its splitting field E/F, then there is an automorphism $E \to E$ fixing F sending α to β. In particular the automorphism group of E fixing F permutes the roots of $f(x)$ transitively.

Proof of the extension theorem

The proof is by induction. If all roots of $f(x)$ belong to F, then all roots of $f'(x)$ belong to F', and $E = F$ and $E' = F'$ so the identity map works. Now suppose we know the result for all f of degree less than n and suppose that f is of degree n. Choose an irreducible factor $p(x)$ of $f(x)$ of degree at least 2, and the corresponding factor $p'(x)$ of $f'(x)$. Since $F[x]/p(x)$ is isomorphic to $F'[x]/p'(x)$, we have an isomorphism
$phi' : F(\alpha) \to F'(\beta)$ that restricts to $\phi : F \to F'$.

Let $f(x) = (x-\alpha)f_1(x)$ and $f'(x) = (x-\beta)f_1'(x)$. Now E (resp. E') is a splitting field for f_1 (resp f_1') and by induction we have an isomorphism $\sigma : E \to E'$ that restricts to $\phi' : F(\alpha) \to F'(\beta)$. This σ also restricts to $\phi : F \to F'$ (since ϕ' does).

Another property of splitting fields

Proposition: Let K/F be the splitting field of a polynomial. Then if $g(x) \in F[x]$ is any irreducible polynomial over F, and $\alpha \in K$ is a root of $g(x)$, then all roots of $g(x)$ belong to K. (In other words, if K/F is a splitting field for some polynomial, then any polynomial in $F[x]$ is either irreducible or splits into linear factors over K.)

Proof: Suppose that K is the splitting field of $f(x) \in F[x]$. Suppose that $\alpha \in K$ and let β be another root of $g(x)$ and consider the field $K(\beta)$. Then $K(\beta)$ is the splitting field of $f(x)$ over $F(\beta)$. (K contains all the roots of $f(x)$, and it must contain β if it contains $F(\beta)$.) But then we have the diagram:

$$\begin{tikzcd}
K \arrow[r] & K(\beta) \\
F(\alpha) \arrow[u] \arrow[r] & F(\beta) \arrow[u]
\end{tikzcd}$$

The extension theorem tells us that there is an isomorphism from K to $K(\beta)$ carrying $F(\alpha)$ to $F(\beta)$ and fixing the field F. Therefore $[K : F] = [K(\beta) : F]$. But then

$$[K(\beta) : F] = [K(\beta) : K][K : F].$$

This forces $[K(\beta) : K] = 1$ so $\beta \in K$.

Algebraic Closures

Algebraic closure

Definition: A field F is algebraically closed if it has no nontrivial algebraic extensions; in other words, if every irreducible polynomial over F has degree 1.

Definition: If F is a field, then $\overline{F}$ is an algebraic closure of F if $\overline{F}/F$ is algebraic and every polynomial in $F[x]$ splits completely in $\overline{F}$.

So notice that the complex numbers are algebraically closed, but they are not an algebraic closure of $\mathbb{Q}$, because they contain transcendental elements.

Algebraic closures are algebraically closed.

Lemma: If $\overline{F}$ is an algebraic closure of F, then $\overline{F}$ is algebraically closed.

This lemma says that if every polynomial with coefficients in F has a root in $\overline{F}$, then every polynomial with coefficients in $\overline{F}$ has a root in F.

To prove this, let $f(x) \in \overline{F}[x]$. Let F_1/F be the extension of F generated by the coefficients of f. Since F_1 is generated by finitely many algebraic elements, F_1/F is finite and a root α of $f(x) \in F_1[x]$ is finite over F_1. Therefore f has a root in a finite extension of F, which is therefore in $\overline{F}$.

Every field has an algebraic closure

Theorem: Given a field F, there exists an algebraically closed field containing F.

Proof: See Proposition 30 in DF on p. 544.

Theorem: If K/F is algebraically closed, then the collection of elements of K that are algebraic over F is an algebraic closure of F.

Since $\mathbb{C}$ is algebraically closed, the set of algebraic numbers inside $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$. The construction of $\mathbb{R}$ and $\mathbb{C}$ is primarily by analysis, and the proof that $\mathbb{C}$ is algebraically closed is also analytic – at least, the usual proof.

Separability

Separability is a phenomenon that is important when studying polynomials over fields of characteristic p.

Definition: A polynomial is *separable* if it has distinct roots, and inseparable if it has repeated roots.

Proposition: An irreducible polynomial over a field with characteristic 0 is separable. It is inseparable over a field with characteristic p if and only if its derivative is zero.

Proof: If α is a repeated root of a polynomial $f(x)$, then $f'(\alpha) = 0$ where f' is the "formal derivative" of f. Conversely, if α is a common root of $f(x)$ and $f'(x)$, then α is a multiple root of $f(x)$. This is because of the product rule; on the one hand:

$$\frac{d}{dx}((x-a)^r g(x)) = r(x-a)^{r-1}g(x) + (x-a)^r g(x)$$

so if a is a multiple root, then it is a root of $f'(x)$. On the other hand, if a is a common root of $f(x)$ and $f'(x)$, write

$$f(x) = (x-a)g(x)$$

so

$$f'(x) = (x-a)g'(x) + g(x).$$

Since $f'(a) = 0$, we have $g(a) = 0$ so $g(x)$ is divisible by $(x-a)$.

Now if $f(x)$ is irreducible, then since $f'(x)$ has degree less than $f(x)$, if it is nonzero it is relatively prime to $f(x)$. In characteristic 0, it is automatically nonzero. In characteristic p, it could be zero. For example the derivative of $x^p - a$ is zero.

Notice that if a polynomial has derivative zero (over a field of characteristic p) it must be a polynomial in x^p. From this one can see that any irreducible polynomial $f(x)$ over a field with characteristic p is of the form $f_0(x^{p^k})$ for some power of p, and $f_0(x)$ is a separable polynomial.

The Frobenius map

If F is a field of characteristic p, then the map $\phi : F \to F$ given by $\phi(x) = x^p$ is a field endomorphism called *the Frobenius map* or *the Frobenius endomorphism*.

If the Frobenius map is surjective, then evey irreducible polynomial over F is separable. Such a field is called *perfect*.

View as slides